Tertiary Education Commission
Te Amorangi Mātauranga Matua

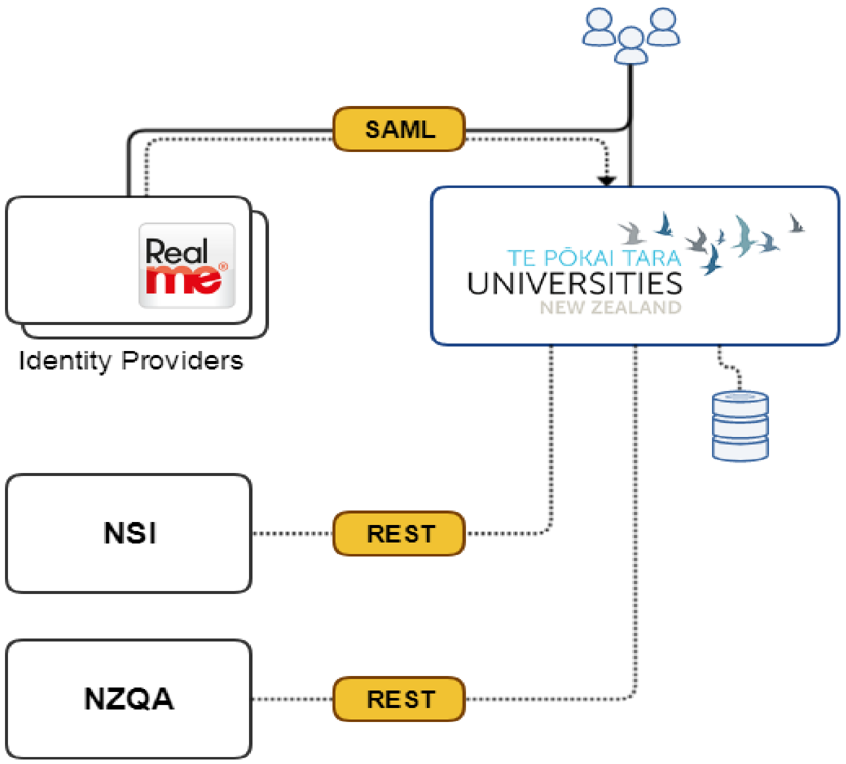
University of Auckland's Online Application for Admission: A guide to how we set up our prototype

The University of Auckland prepared this guide to share their experience and lessons learned. You may find these helpful as you consider setting up your system.

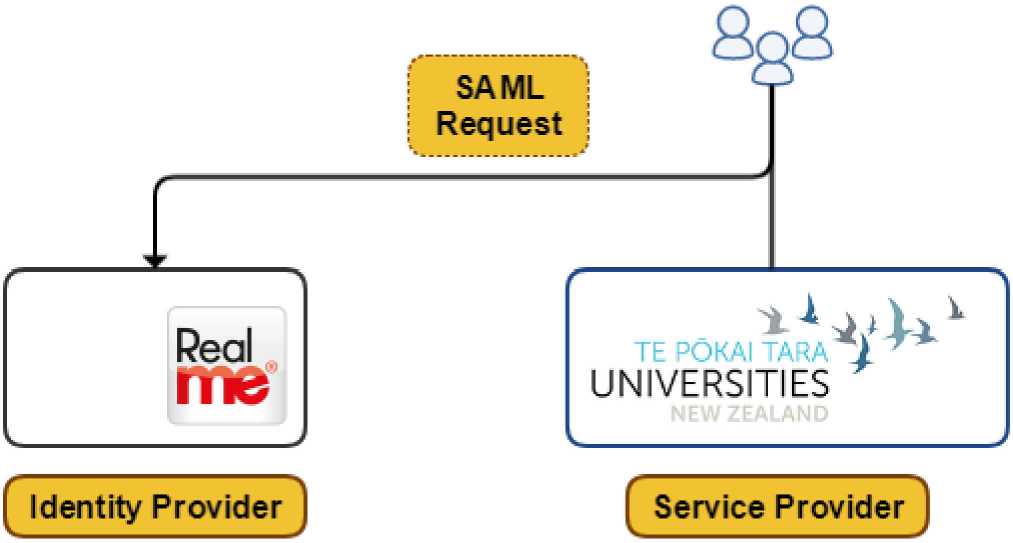
The steps in the process

1. Integration with RealMe® for identity verification
2. Integration with the Ministry of Education National Student Index for NSN
3. Integration with NZQA for achievement record

Diagram of how it works



Integration with RealMe®



Integration with RealMe® is based on SAML2. This requires two participating organisations (RealMe® acting as the *Identity Provider* and the integrating institution acting as the *Service Provider*) to exchange certificates and metadata before any SAML interaction can happen. These integration steps vary between environments.

RealMe® has three environments: MTS, ITE, and PRODUCTION

MTS – sandbox:

1. Follow documentation here (link), download the start-up pack, and construct the valid metadata file based on the sample metadata and sample certificates.
2. Upload the new metadata to RealMe® through the website (link).
3. Configure your preferred SAML2 library to use the metadata file created earlier.
4. MTS is a sandbox and it does not have any identities stored in it. Each time authentication is initiated, RealMe® MTS will prompt a user to enter the data to be returned as attributes.

ITE – test environment

1. Acquire SSL certificates for your organisation (confirm the technical, naming-convention, and certifying-authority requirements with RealMe® through the website (link))
2. Generate new metadata, and prepare your logo, welcome, and error messages.
3. Contact RealMe®/DIA to configure your application/system with RealMe® ITE environment (including exchange of metadata, certificates, and logo/messages).
4. This environment is technically equivalent to the real production environment, and it supports two-factor authentication. Security (SMS) codes for testing can be accessed in real time here - link.

Production

Contact RealMe® to setup your application/system. Overall, the steps to achieve this are the same as for the ITE environment:

1. Acquire SSL certificate for your production environment
2. Generate new metadata

3. Contact RealMe®/DIA to setup your production application

Assertion vs Login

When the Service Provider (SP) initiates a login with RealMe®, it can specify whether it should be an Assertion or Login. The difference is that with Login the only information returned to the SP is user's login identifier (Federated Logon Tag - FLT). To receive a user's attributes (such as Name or Date of Birth), an Assertion is required.

- If the user is already registered with the organisation, use Login and lookup the user's identity in the local store by FLT
- If you need to register, use Assertion and save this information into a local store along with the FIT (Federated Identity Tag) and FLT.

Helpful resources

https://www.samltool.com/online_tools.php

https://mts.realme.govt.nz/realme-mts/request/validator.xhtml

Integration with Ministry of Education National Student Index

Contact NSI to provision API access credentials:

- Username
- Password
- Scope
- Organisation ID

These credentials are used to dynamically provision *access_token* and *session_token* for accessing API endpoints.

TEST endpoints:

https://ppsecurity.education.govt.nz

https://nsi.compliance.education.govt.nz/api/V1

PROD endpoints:

https://security.education.govt.nz/

https://nsi.education.govt.nz/api/V1

Step 1 - Access Token

Provision *access_token* using standard OAuth2 Client Credentials grant. Example Request and Response below. Username and password are used to generate authorisation header, also Username is passed as a parameter to the Authorisation endpoint as shown below.

Request:

Header	*Authorisation: Basic {base64-encoded-credentials}*
POST	https://ppsecurity.education.govt.nz/oauth2/access_token?grant_type=client_credentials&end_user_id={USERNAME}&scope=APP_NSI2

Response body:

```
{
  "token_type": "Bearer",
  "access_token": "TOKEN"
}
```

Step 2 - Session Token

Exchange access_token to session token (returned in headers)

Request:

Headers	*Content-Type: application/json,* *Accept:application/json*
POST	https://nsi.compliance.education.govt.nz/api/V1/session

Body	{
	"ESAAAccessToken":"*TOKEN*",
	"OrgId":*ORG_ID*
	}

Response header:

```
NSISessionToken: bf671965-39dde71cf605
```

Step 3 - call API example

Use session token to invoke API endpoints. If the session token is expired, refresh the session token by repeating Step 2.

Request:

Headers	*NSISessionToken:{},* *Accept: application/json*
GET	https://nsi.compliance.education.govt.nz/api/v1/student/126986469

The example above shows how to access student information by their NSN. In the context of RealMe® authentication NSN is not available and needs to be looked up using NSI *search* endpoint and Name + Surname + DateOfBirth from the RealMe® Assertion payload.

Integration with NZQA

NZQA is using standard OAuth2 Client Credentials grant to authorise access to APIs.

Contact NZQA to provision *client_id* and *client_secret*. Example *scopes* include:

- learner_achievements_private_read
- learner_courseendorsements_private_read
- learner_scholarships_private_read
- learner_standards_private_read
- learner_quals_private_read
- learner_profile_private_read

OAuth2 token endpoint in test is: https://api-test.nzqa.govt.nz/token

Example retrieving qualifications in TEST:

Headers	*Authorization: Bearer {OAuth2 access_token},* *Accept: application/json*
GET	https://api-test.nzqa.govt.nz/learners/v1/{NSN}